Privacy & Security Standards Workgroup
Draft Transcript
January 26, 2011

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you, Operator. Good afternoon and I guess I should say welcome back, everybody, to the Privacy & Security Standards Workgroup This is a Federal Advisory Committee, so there will be opportunity at the end of the call for the public to make comment.

Let me do a quick roll call of members. Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Walter Suarez?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Anne Castro? Steve Findlay? David McCallie? Sharon Terry?

Sharon Terry – Genetic Alliance – President & CEO
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Steve Ondra or Chris Vane? John Moehrke?

John Moehrke – Interoperability & Security, GE – Principal Engineer
I am present.

Judy Sparrow – Office of the National Coordinator – Executive Director
Sue McAndrew? Ed Larsen?

Ed Larsen – HITSP
Present.

Judy Sparrow – Office of the National Coordinator – Executive Director
Kevin Stein? John Blair?

John Blair – Tacanic IPA – President & CEO
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Did I leave anyone off? Okay. With that I'll turn it over to Dixie Baker.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. Thank you, all, for joining us today. It's been a while since our Workgroup has convened. As you know, the Standards Committee received a request from the Policy Committee to develop/recommend

standards for certification and certification criteria for digital certificates to be used in authenticating organizations who are exchanging electronic health records. So today we are launching our discussion about digital certificate standards and I've asked Walter Suarez, our new Co-Chair, to lead this discussion. So with that, Walter, can you take it from there? I think we have these slides; they are available on the Adobe Connect and I think Judy Sparrow – I'm sure Judy Sparrow sent them out earlier this morning. So, Walter?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. Thank you. Thank you, Dixie. Welcome, everyone, again to this first meeting of our Workgroup this year. We have put together a series of slides. Let's go to the next slide and go over the agenda of what we wanted to do today. We basically wanted to do a review, first of all, of the HIT Policy Committee recommendations on provider authentication and digital certificates just to get us all on the same page with respect to all of the recommendations; then review specifically the directions and the recommendations that came back to the HIT Standards Committee on digital certificates. Then we'll take us all through a quick, technical review and background of the concepts, the key concepts around digital certificates. We'll talk about PKI and all of the elements that are needed to be covered around digital certificates and then discuss the approach that we would be following with respect to the recommendations. We'll highlight some of the standards that exist and talk about how we're going to be identifying, evaluating and then selecting the standards that we would recommend for adoption. Then we close off with some timeline and next steps, you know, when do we see we would be completing this task and what are some of the next steps that we would take.

The presentation, I should say, includes already a glossary of terms that we will be referencing a little bit later, but at the end of the presentation we included a glossary of key terms just to get us all also on the same page of many of these terms that are used, that are associated with digital certificates. So we'll reference those as we go along here.

The next slide: So let's start with the recommendations from the Privacy & Security Tiger Team and then approved by the Policy Committee. Just to frame this, as you probably have seen from the letter of the Policy Committee to the National Coordinator, basically, they kind of frame things in the sense of they wanted to establish a trust of framework for information exchange between healthcare providers and patients and create a high level of assurance that an organization exchanging health information is who it says it is basically using digital certificates.

They didn't include or they didn't want to focus their attention directly onto the individual level, digital certificate and level of assurance, but to try to focus this initial set of recommendations on organizations exchanging health information at the organization level of digital certificates. So that's another consideration in the recommendations.

Next slide: We'll just start with the series of recommendations and we'll go through all of them. The first one, this specific one is the one that directly relates to the work we're going to be doing, but we thought it would be important to cover these other ones as well. Recommendation number one that they made is about which provider entities should be issued digital certificates. They pointed that all entities involved in healthcare exchanges will be expected to obtain and have a digital certificate to use in exchanges. Sort of examples of these entities would include the list that you see on the slide: Covered entities; business associates; personal health record providers; public health entities; pharmacy benefit managers; retail pharmacies. All of these groups and entities are expected to have, obtain and use a digital certificate when exchanging health information.

Next slide: The second recommendations focus on requirements to be issued a digital certificate. Organizations seeking digital certificates must demonstrate that, first of all, they exist as a legitimate business or have a valid business or is a valid business entity, a legal business entity. To demonstrate that they can use things like a valid licensure, business licensure, a business proof of address and corporate existence, a financial account. Those kinds of elements would be used to demonstrate that they're a business. And that they also participate in electronic exchange of healthcare information.

Those are two conditions that they recommended would be requirements for entities to be issued digital certificates.

Credentialing organizations or certificate issuers would then rely on existing criteria and processes for verifying and confirming the legitimate existence of entities, for example, using the National Provider Identifiers and other types of numbers like that that verify and confirm the existence of entities.

The Policy Committee did not seek to impose additional privacy and security requirements of provider entities seeking certificates at this time. They basically assume privacy and security accountability infrastructure would be developed by the Governance Workgroup of the Policy Committee and that would then be the requirements that govern this entity seeking certificate.

The next slide is the third recommendation and it focuses on the process or completing the process for issuing digital certificates and for re-evaluations. Multiple credentialing entities will be needed to support this process of issuing and releasing digital certificates considering the number of healthcare entities that would be expected to obtain them. So they gave a few examples; vendors and state agencies might become authorized issuers of certificates. They should also leverage existing processes, such as a federal bridge and entities such as health information organizations that are operating regional health information exchanges. It would be also entities that could play a role in becoming issuers of certificates.

It points also to, in this particular recommendation, that certificates should contain an expiration date requiring renewal at least yearly of when there is a material change in the evidence originally submitted to justify the issuance of a certificate. So there is an expectation of the content of the certificate and, as we'll talk about, that's one of the requirements or one of the expectations on the Standards Committee, to make recommendations about the content, the data elements that form the data for the certificates. So we'll talk a lot more about this a little later.

The next recommendation, recommendation number four; the next slide, please; talks about the characteristics of who can credential or issue the digital certificate. So they point out to any entity willing to assume the related risk of being held accountable for providing and confirming the high level of assurance and accuracy that is needed and that meets the established standards for issuing certificates will be able to become a digital certificate issuer. The Policy Committee recommended that ONC establish an accreditation program for reviewing and authorizing these issuers of certificates with an annual credentialing; well, they pointed out that annual credentialing of these entities might not be enough; that credential issuers must be required to operate with transparency so their operations can be monitored and problems can be quickly identified and addressed. This requirement for accreditation should be continuously evaluated in the process of the recommendations of the Governance Workgroup related to governance of health information exchanges. That was the recommendation related to the issuers of the certificates.

The next slide, slide number five or recommendation number five; this one is certainly the one that specifically points to our Committee, our Workgroup. This recommendation notes that ONC, through the Standards Committee, should select or specify the standards for digital certificates, including the data fields, in order to promote interoperability among healthcare organizations. It also notes that EHR certification should include criteria that tests the capability of EHRs to be able to retrieve, validate, use and revoke digital certificates and that are expected to comply with these standards being defined as a committee.

It noted also the Policy Committee leads this recommendation to standardize provider certificates and to establish the certification criteria represents an important component to achieve the interoperability and the greater interoperability between healthcare entities exchanging health information. So they see it and they thought that we have a critical component in this process of achieving greater interoperability.

The next slide, slide number six or recommendation number six, is the final recommendation. Very briefly, it talks about the types of transactions requiring certificates. It points out the fact that authentication is going to be required on any transaction when the content of the exchange must be

appropriately protected due to the content itself having personally identifiable or individually identifiable health information. Also, when the identity of the sender and/or the receiver must be known and validated and in some cases they only need to authenticate one end of the exchange instead of both.

It provides also a few examples of transactions that may require authentication: Sending and receiving transactions that contain individually identifiable health information or that may otherwise pose a risk to the patient if the information is not protected appropriately. Transactions that would normally be authenticated outside of healthcare; on bulk transactions used to transfer multiple patient records with identifiable health information; for example, within transactions that they see would require this authentication of both the senders and receivers.

Let's see. I think those were the recommendations. Let me stop there and see if there are any general questions or comments or reactions to the recommendations that would be helpful in our diving into the discussion of standards. Any questions or comments?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, Walter. This is John Moehrke.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, John. Go ahead.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes. I think these are really good recommendations and I guess maybe my question is more on what's next, so to speak. How are we to interpret these? Because I think there's a few things that are worded in here that I think if we understand them as high-level policy as opposed to technology choices it may be easier to understand when we pull out one specific and I think it will be instructive.

In item number three there is requirements to have an expiration of one year, which, at the technology level can be interpreted as literally one year, but that will ultimately produce a very shabby and frail infrastructure, but I think the intent there is to have a policy that can react to the needs of changing identities and changing trust networks as opposed to explicitly saying one year. I see a couple of other things within some of the other recommendations that I'm not sure whether the intent there is to be as technology prescriptive versus guidance.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. Well, that's an excellent point. Clearly, these were policy prescriptive more than technology prescriptive, so in the case that you're pointing out I think the expectation of having the expiration date of the certificate be at least yearly to renew, require to be renewed at least yearly somehow, not less, later I guess, than once a year or when there is a material change to the issue that got issued the certificate, those two conditions. I think those were policy-level decisions and recommendations. If that or if those kinds of recommendations effect the recommendation of the technology itself then that's something we would need to discuss. In so far that they protect how or which type of technology standard or recommendation we select that would be an important point to highlight.

I assume that if we find those kinds of specific issues, certainly we can go back to the Tiger Team to help clarify and help define whether those specific policy driven recommendations of things like renewing every year or ... had a specific meaning that cannot be affected by virtue of the technology being different or forcing a certain level of technology decision. So I think we can go back certainly to the –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
May I make a comment about this, Walter?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Sure. Go ahead. Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie Baker. The chattiness has to do with how often you query for whether the certificate has expired or not. The question of how often you need to renew it is a policy question and not a standards question. The standards question is how we persist the expiration date in the certificate itself. So I think we really need to focus on what the standards for the digital certificate are. We are not charged with coming up with policies on how often an application needs to check it or any of the others. I mean Walter has shown us the full context of the recommendations ... that we do have. Here is where the digital certificates fit into the scheme of things, but this working group's charge is to really recommend standards for digital certificates and those standards need to include the data fields; that includes the expiration date; but we aren't charged with deciding how often you check to see whether it's expired or not. So –

(Overlapping voices.)

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
... go ahead, John.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, the standards I don't think are a problem choosing them. What I'm bringing up is, for example, with the NHIN Exchange there was actually an even tighter prescriptive line very similar to this that when they looked at the standards the standards could support it. It wasn't a problem of whether the standards could support. What the result of combining the policy with the standards with the realities of how they were going to be used became an operational impossibility –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right and I'm not refuting your point at all. But the point is it's a policy issue that I think is not the work of this working group. I would encourage you to bring that issue up with the Tiger Team and not this working group.

(Overlapping voices.)

John Moehrke – Interoperability & Security, GE – Principal Engineer
I think ... was the way that we can communicate those issues to the policy people as we find them –

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Exactly. I think what you're saying, John, and I think we can proceed that way is as we look at the standards, which is the scope of the Workgroup, and we find that there are potential implications to some of the policy recommendations they made in other sections of the recommendations we should bring those apps back to the Tiger Team.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, that's what I was looking for thank you.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I just don't want to go in a direction – I would prefer that if we have policy that we not get really wrapped around the axel, on operational implications of the policy and that rather we really keep a tight focus on the charge that's been given to us, which is to specify the standards.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
No. Yes. Dixie, I think we will. We will keep a very tight focus on the standards. I think that's the charge and the fixation that we have, but I think to John's point, if we find that for a particular reason by going down a standard and considering the other policy points that were made, the other policy recommendations were made, there is a ... possibility, as John has pointed out in the example with –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, it's not ..., but let's –

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
But actually, one year is not too bad.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, it's not an impossibility. Let's just go ahead with the discussion, Walter.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Walter?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. Go ahead.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is David McCallie. I'm late to the call. I just wanted to let you guys know I had joined in. Unfortunately, I'm going to only be able to stay for a little while, so I'll stay as long as I can and look forward to it. Thank you.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay. Great. Thank you.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Thank you.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
So we're going to go to the next slide and we're going to basically highlight the focus of our Workgroup. Again, the primary focus is to select or specify the standards for digital certificates and then define the standard data fields and content requirements of the certificates. We would also point to the fact that we would be defining the EHR certification criteria that ensures EHR is going to be capable of retrieving, validating, using or revoking digital certificates. Those are sort of the three main elements, the standards for digital certificates, the data content, the data fields and then the EHR certification criteria that would go along with it.

We're also going to focus on organization-to-organization exchange, what is known or we call Class 2 and Class 3 digital certificates, entity level, as well as software level certificates. We will not define standards for individual person level digital certificates. We have to certainly consider all of the other policy recommendations in defining these standards for digital certificates that so far just basically, even though we're going to focus certainly on number five, recommendation number five, we have to take into account and consideration the other recommendations as we look at the standards for data fields and the certification criteria.

So any questions or comments about that?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, I have a question just to validate: The fourth bullet there is really my personal interpretation of what we need to do and I would like some discussion or confirmation or disagreement or whatever. My feeling is that if we're going to specify standards for digital certificates to support the exchange of clinical information between organizations that a Class 2 is not sufficient; that you really would need to go one level deeper and do the software, Class 3, certificates as well. Do you guys agree with that?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Any reactions to that point?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. Maybe I better clarify. The Tiger Team had considerable discussion, as David McCallie certainly knows, about whether an organization has a single entry point. I think we all know that that's not realistic and the Tiger Team knew that as well. So the Tiger Team acknowledged that a single organization could have multiple entry points and that's why I made that cognitive leap to assume that we would then need – if there are two different servers that you can use to exchange information with an organization it seems to me each server should have its own certificate.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is David. I was on mute before. That makes sense to me. I think the spirit of the discussion in the Tiger Team was clearly to focus on whatever it takes to have meaningful security at the organization level, but not to worry about it at the individual level. If organizations are complex entities then the certificates would have to reflect that complexity.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's my feeling as well. I just didn't want it to be an assumption.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. It makes sense to me. I'm not sure I know what the technical consequences of that are. Maybe that will come out as we get deeper into it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It has to do mostly with that you need to do to prove your identity to get it, you know?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
... came up with the class structure that pretty much everybody uses I think now.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. In fact, I mean I would agree with that. Those are the two levels or classes I think that we would be focusing on. As we will talk a little bit later, there are two other ... that are much more specific to certain types of businesses ... so I think you're right. I think those will be the right levels to focus on.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes. This is John. I think I agree with you in spirit. The question becomes whether there is organizations for which the software level is really unnecessary. I'm not sure whether I have a clear understanding of when that would actually be. It seems to me even a small organization that only has one interface that could be a software level –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. I agree. I think that's a policy issue.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, but I think the complexity comes with looking at all of the potential interfaces, for example, the direct project is a decidedly different kind of an interface. I don't know whether that necessarily drives your question one way or the other.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay. So if we get to discuss in more detail the recommendations of the type of standards and then put it into the context of the project, such as the direct project or exchange or others, we can play it back and see how this Class 2/Class 3 will work or whether we focus or refocus on only one or continue both.

All right. So let's go to the next slide. I think here we're getting to, I guess, the start of a technical review and background on some of the key concepts. Most of you are quite familiar with these, so ... so we'll just review. I think it was important to put together something that we will all feel comfortable and helpful about ... kind of the same level of understanding when dealing with complex concepts, because some of them are pretty complex. So when thinking about digital certificates there are a number of other critical concepts and elements and parts and aspects of securing information exchanges and so we thought of highlighting a few of them and we'll talk in some more detail about a couple of them.

When dealing with digital certificates you have to talk about Public Key Infrastructure, the public key and private key kinds of concepts, the definition of digital certificates, the role of other things, like digital signatures and encryption in this process and then all of the infrastructure elements needed to support this type of securing of messaging, certificate authorities, certificate policies, registration, authorities, all of these elements, certificate revocation lists and things like that. So we've put together, as I mentioned, at the end of the presentation a glossary of terms to have as reference in all of our discussions and kind of have in the background, so whenever there is a question about what do we mean by public key or private key or encryption or certificate authority or this or that we have a reference.

The glossary, by the way ... reference in this slides that include the glossary comes out of the NIST publication on the introduction to PKI. I think we can probably include some reference, video-graphic reference materials that will be helpful for people to have if they want to read and understand in more detail some of these concepts. So we'll probably add that to the items that we disseminate along with this glossary.

Anyway, those were some of the key terms that we always have to and we will be dealing with in more detail. We'll dive in the next few slides into some of the specific concepts to help us again understand what is public key infrastructure, what is digital certificate.

So let's go to the next slide and talk about some over arching concepts. So basically, when you start thinking about security mechanisms that are ... to secure and achieve authentication and non-repudiation and integrity and all of those core security concepts, there are two major groups for the security mechanisms that one has to think about. The non-cryptographic security mechanisms or mechanisms that certainly do not use cryptographic methods and examples of those are the parity bits or the digitized signatures; not digital signature, but digitized signature, basically a scan of a paper signature. Having PINs and passwords and biometric measures are examples of non-cryptographic security mechanisms.

Then there are cryptographic security mechanisms, which are involved much more specifically in the exchange of messages that need to be protected, so there is symmetric keys, like the AES. There is secure hash and then there is the asymmetric cryptography, which is basically the foundational concept of public key and public key infrastructures and digital certificates. So that is sort of where the recommendation from the Policy Committee sits is in this last item of directing us to develop standards and identify and recommend the standards for digital certificates, which are asymmetric, cryptographic methods of secure messaging.

All right. Let's go to the next slide to begin to sort of focus more into this concept of public key cryptography. Basically, the concept here; and, Dixie, I think this is your picture, so I hope I'm going to relay this appropriately; but basically the concept is that a sender is going to be sending a message to a receiver and they need the message to be protected basically and so there is going to be a couple of things around that. First, the message, which was originally in clear text needs to be converted, if you will, into some cipher text that will protect the message. So the, "Hi, Bob," needs to be converted into this cipher text that protects the content of the message.

Then the receiver of that message – so in order to do that there is a generation of a key on the sender side that ensures that the clear text message will then be sort of protected or converted into the cipher text. Then the receiver of the message needs a key in order to basically decrypt and turn this cipher text back into a clear message so they can see it again. That's sort of how the public key/private key mechanism of protecting the content of a message works basically.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Walter –

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Dixie, do you want to say some things about this? Go ahead.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Walter, you know, I sent you these kind of basic elementary diagrams to level set in case some of the people that called in for this discussion were not familiar with digital certificates and asymmetric encryption. I think I heard all of the names. I think most of the people on the call understand this. Is that correct? If I'm correct there maybe we could cover these pretty quickly.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. Let's see. Is there anyone on the call that doesn't understand the basic concepts behind asymmetric cryptography and the public key infrastructure? Anyone?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. So why don't –

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. Why don't we go ahead and move a little faster then in this section? So the next slide talks about the uses and I mentioned authentication basically, making sure that a message encrypted with public key can only be decrypted by an authentic owner of a private key. Non-repudiation is the other element that's supported by public key and then integrity protection. Those are the three security elements supported by public key cryptography.

The next slide –

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Walter?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is David. I wanted to ask a question. These slides to me imply that we're talking about encrypting the message rather than the channel. Have we made that decision or is that an irrelevant question at this level?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It's relevant at this level, but if we're talking NHIN Direct, obviously, it is message oriented, but I think our charge is really to specify standards for digital certificates, whether they be used for digitally signing something or encrypting, exchanging a symmetric encryption key for TLS channels.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Got you. That's helpful. Thank you.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. Okay. So the next slide –

John Moehrke – Interoperability & Security, GE – Principal Engineer
...

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I'm sorry?

John Moehrke – Interoperability & Security, GE – Principal Engineer
... clarification I believe it is for communications, not for long-term digital signatures.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Okay. Because that is, I think, a logical carve off; long-term digital signatures have the same technology, but have very different requirements –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Very.

John Moehrke – Interoperability & Security, GE – Principal Engineer
... 20-year or 30-year or 40-year ...

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Excellent point and we should make sure that we state that in our assumption. That's a great point, John.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
That's a great point. That's exactly it. Very good.

John Moehrke – Interoperability & Security, GE – Principal Engineer
But I do agree we should be able to resolve the issue of identity assurance for communications, whether they be transport standards, such as TLS, or messaging standards, such as S/MIME.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. Yes. We think about the NHIN Direct model. It uses a digital signature, but it's not this type of long-term digital signature. That's a really good point.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Great. Thank you.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Great. Okay. So let's continue this and again, we'll go through the next few slides fairly quickly. The next slide just defines what PKI is. We all sort of understand all of this framework for the generation, distribution, management, certification and revocation of public keys. There are some enabling technologies for secure e-mail, digital signatures, secure Web access, secure exchanges of secret keys.

Let's go to the next slide, Digital Certificates. Since we are required to come up with recommendations on standards we thought it would be important to focus the attention a little bit on the definition of that and so here is sort of the definition of digital certificates. Again, this is coming out of the NIST publication, but it's generally speaking, a most accepted definition. It is a digital representation of information that has at least these five characteristics: Identifies a certification authority that issued the certificate; identify the names or include the names of the subscriber; contain the subscriber's public key; identifies its operational period; and is digitally signed by the certification authority that is issuing it. So those are five key characteristics of a digital certificate.

We talked about the classes of digital certificates. There are five classes generally kind of agreed on. Class 1 focuses on individual levels of digital certificates. These are certificates for individuals, assigned to individuals and mostly intended for use with e-mail.

Class 2, as I say, are certificates assigned to identify organizations, so entity level.

Class 3 is certificates issued to identify servers and for software signing.

Then there is Class 4, which are certificates for on-line business transactions between companies and Class 5 certificates for private organizations or government and security. Those are more specific levels or classes of certificates.

They can exist in different formats. The most popular, most common standard used is the standard developed by the ITU Telecommunications Standardization Sector called X.509, which specifies that standard formats for the public key certificate and also the algorithms for the certification of path validation. So certainly we'll be talking more about this particular standard later on. So those are just basic concepts about digital certificates.

The next slide highlights the common content elements, the most common content elements of digital certificates. This is coming out of the X.509 standards. So a Serial Number that is used to identify uniquely the certificate.

There is a Subject or the name of a person or entity to whom the certificate was issued.

The Public Key itself of the certificate owner.

There is a Signature Algorithm, the algorithm used to create the public key.

The Issuer, the name of the certificate authority and the Issuer's Signature.

Then there is Valid-From and Valid-To, the day the certificate is first valid and then the expiration date.

A couple of other elements: The Key-Usage, basically the purpose of the public key that is to be used for things like encipherment or signature.

Then the URL of the certificate revocation list and a couple of other items, the Thumbprint Algorithm, the algorithm used to hash the certificate and the Thumbprint itself, the hash itself.

Those are some of the most common standard kinds of data fields or data content elements in the certificates. We'll use that as a reference in sort of drafting our recommendations, but we wanted to just put it in here as a starting point of discussion.

So let me stop there and see if there are any questions or comments on this last couple of slides, the definition of digital certificates or the data fields. Any comments?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Walter? Walter?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. Go ahead.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is David. Are there other fields that are in common use or is this the total subset that's covered? I mean I'm questioning around the definition of who the subject is. Is it allowed to specify in some detail who the subject is or is it a single string, for example?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Well, I think personally there are some other data elements that are, I guess, not required, if you will, that are optional data elements that have been in some cases used. We didn't list them here. That's one point. There might be other data elements that have been used and I don't have examples of those, but that's one thing I found out anyway; that there are some.

Then with respect to the content definition of these data fields themselves and the degree to which they are defined in the center I think, for example, in the one that you're looking for, the subject, I think the definition of the standard is fairly generic. It's sort of just framing this is the name of the person. That's my understanding, but maybe others have a different understanding.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie. Several years ago I was involved in the Automotive Network Exchange, the ANX network. As I recall, we specified very detailed data elements within each of these big fields. If I could find that specification I could maybe share it with people so that they could see what it looked like, but subject was not like an empty field that you could put David McCallie or McCallie,David or whatever you wanted. It was precise, like we specify an HL-7 message, like we should be specifying HL-7 messages.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
And that would be my guess as to what kinds of things they want us to recommend back –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. I think –

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Explicit details at that level.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. That would be my understanding too.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Got you.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
And I would expect that we would use to reference standards that we would be identifying, for example, the X.509 and the description in that standard of the definition, the detailed definition of the content of the field.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, we've used X.509, but I mean in X.509 it's kind of like HL-7 Version 2 where you have specified fields, but you have a lot of flexibility in establishing how the fields, the information the fields are represented and I think that's what we need to do.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Right.

John
Okay. And the fields you have shown here are for the most part the mandatory fields. There certainly is room for optional and within a particular exchange there may be some reason to add optionals. I think that will be more likely the case when you're using a transport like the direct project than it would be for machine-to-machine certificates. So I think that may also be some place where we get prescriptive about one kind of use versus another kind of use, but I think we need to have some recommendation in the first place.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. I agree with you.

John
I think another thing, David, you may be trying to get at is something we did run up against in the direct project where a certificate is an organizational certificate that is good for some N number of e-mail addresses and that is indeed playing some tricks with the subject value, but I think we can certainly learn from what the direct project learned from there.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, that's kind of what I had in mind and also just the complexity of some of these multi-facility organizations, particularly if they become accountable care organizations and they might actually span multiple covered entities. It's not going to be trivial to decide how to even identify yourself, much less what we codify in the subject field.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

John
Yes. Again, the requirements are likely more simple for TLS because it's machine-to-machine than it would be for a messaging .... A lot of that also has to do with something we haven't talked about yet and that is the separation of identity and authentication of that identity from the authorization of what they're allowed to do. I've seen many mistakes made on trying to combine those and say, "Well, gee, anybody who has a certificate issued from this root is authorized to do all kinds of things." It's like, no, they're just identified. The authorization is a second step.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. My understanding is that we are, I mean based on the recommendations from the Policy Committee, we're really focusing on authentication. We're not –

John
Correct.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Tying the authentication part to any particular authorization and so to your point, yes, I think we've got to keep that in mind and not go down that path of linking the authentication ... with any particular authorization and ....

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is David. I agree with that totally. It's a slippery slope that a lot of people fall into, as John points out –

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Because you think if I can prove that you couldn't have gotten the certificate unless you proved you're a doctor then I'm going to authorize you to act like a doctor, but it's really two separate things.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie. Does NHIN Exchange, have they developed a standard for the digital certificates they use?

M
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That seems to me to be a likely, good place for us to start.

M
Absolutely. Yes. They went through a lot of these imaginations, so it would be useful to pull from them.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Do you know where we would go to get a copy of that? I'm sure it's on-line somewhere, but –

M
I have actually tried to track it down in the past week ... and I do not exactly think I succeeded, so I think we need to ask the leadership for some guidance on finding it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Maybe Doug Fridsma.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I'll check and see if we can pull that out. Judy, we can probably ask ONC's leadership on the NHIN Exchange side to provide us with that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Those are probably Class 5 certificates because it's between government agencies right now.

M
Yes. Again, that got into some interesting –

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Well, it involves government agencies, but it's not only –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right. I know. I know. It's kind of leaking out.

M
Yes –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But it seems to me that if we were to look at use cases to start with that NHIN Direct and sort of informed by NHIN Exchange would be where we would start.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is David. Could I ask a naïve question about these classifications? Is the difference between a Class 2 or a Class 3 or Class 4 just intent of use or is there actually a technical difference between them?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The biggest difference has to do with what you have to present to prove you identity when you get the certificate itself, but I think that there are also policy rules about how often they're renewed and that kind of thing too.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Is that encoded in the certificate so that you can tell what kind of class it is?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. I think, yes. I think so, yes.

M
... related to what certificate roots they will branch to.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. It would seem to make more sense almost to be a root level thing, but it does matter; in other words, it's not just an artifactual categorization.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. It definitely matters, yes. There are standards, like there is a TLS standard that requires – now I can't remember what it is, but it's the latest version of TLS actually requires a Class 3 certificate. We probably could use some more information about the classes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. We can bring in some more details –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. I'll see who I can track down who could really talk to us about the classes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Great.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I agree it would be great to get the NHIN Exchange experience circulated to us so we can learn from that.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. I like the idea of the next steps and when we get to the end of the call the next steps will talk about this. I like the idea of developing a couple of use cases and then learning from NHIN Direct, NHIN Exchange how they're looking at this, what kind of digital certificates they use, those kinds of things.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think NHIN Direct is this will be what will be used in NHIN Direct, but NHIN Exchange is already out there.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, but there is also some experience in NHIN Direct through the pilot projects.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's a good point. Yes. Good point.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So it's not as formal knowledge as NHIN Exchange, but it certainly is worthy to find out. A lot of times you find that there are technical barriers to one choice versus another, so it's always good to pull –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Can you help us track that down, John?

John
Absolutely.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Lessons learned from – okay. Good.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. We can invite also Arien Malec, who directs the NHIN Direct project and hear from him as well. Yes.

Okay. Let's keep going a couple of more slides. I think the next slide, yes, this gets into the certificate generation process. I think we've been talking about the key component of the process of generating a key or a certificate. So there is a key generator, a certificate authority, a certificate revocation list that is

used to reference whether a certificate is active or not. There are other elements that are involved in this particular example, like X.500 and enterprise directories and data warehouses, but I guess generally speaking this tries to represent basically the process of generating a key and using the certificate authority. The certificate revocation list is verified and ....

The next slide highlights the X.509 certificate standard, some of the content elements that have been, I believe, mentioned. So this kind of expands on the elements. I think when we get into the standard again we'll have to do the timing better to learn more data of this data content element, but it's just sort of kind of a graphical depiction of that.

The next slide talks about the V3 extensions of the X.509 standard, the extensions that can be defined by the standards or by the user communities and they include things like alternative name forms, key identifiers, usage, subject attributes, certificate policies, constraints, those kinds of things.

The next slide, I think this slide is the one that summarizes basically the first set, if you will. Actually, if you go back one slide, one more forward; there we go. That one. Thank you. This slide summarizes the standards that are currently available, kind of the first round or the first set, I guess, of standards to consider with respect to digital certificates, the root standards, the IETF, X.509 that we've been referring to and talking about, so there are various reference standards for that.

Then there are the ISO standards, which are much more, I guess, general definition of the standards, so the ISO 17090; that's one that is much more of a basic, conceptual description of the digital certificate usage applied to healthcare and then the 17090-2, which specifies that these are certificate profiles. Those are the two sets of standards that we thought of bringing kind of as a first cut of the standards to consider for digital certificates.

Let me stop there and see if there are any additions or any thoughts or any reactions to this initial list.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think the one that we've identified here today, the standard that we've developed for NHIN Exchange, it's not a standard, SCO type of standard, but it's certainly above an implementation guide and is something we should look at.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay.

M
This is a good list of core standards, but I think there is a set of things above this that we can really leverage as well, like Dixie is pointing out. If the stuff that the Direct project of the Exchange have come up with. There are also things like the VeriSign validation cert. It has some, I think, good information for our target. It has to be, obviously, re-scoped to healthcare, but I know that was one of the things that the Direct project looked a lot at for lessons learned.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Is that VeriSign on the validation cert?

M
The extended validation certificate practice –

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay.

M
You know, the ED certs. When you're at a green bar in your browser there is some really good best practices that have been captured in there and then there's the other pieces about federal PKI that are also important ... contara.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. This is David. That was going to be my question. The federal system uses these approaches quite commonly and we should try to learn from that. We don't necessarily have to match that exactly in terms of maybe some other criteria or the class levels, but there is a huge amount of experience and we should –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But I thought that would be reflected in NHIN Exchange.

M
Yes. Right. I would have guessed.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
It probably is, but it wouldn't hurt. Yes, there is a lot of experience on this federal bridge and this federal PKI activities and it does probably go beyond certainly NHIN Exchange itself, so we will investigate and probably even consider bringing back someone from that project, who will talk to us about what they're doing there.

Any others that people can think of? I mean, John, what do you think about the IHE profile and digital certificate? I know that's ... to the ....

John
Yes. There is not a whole lot in IHE. It's buried within the AETNA profile. They basically find that X.509 technologies are very mature, so there's not much reason to constrain them. I think we will probably have to constrain them further than IHE had to because we actually have a set of policies that we're expected to meet. So we will be more exacting than IHE did, but there are some nuggets in there that we can probably take from, but there are only a few sentences that are really relevant.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay. Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is David. I'm, unfortunately, going to have to leave at this point. I'm sorry I can't stay for the end, but –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, it's past 12:00 or 3:00 your time, so let's wrap it up. I think we have several actions to follow up with.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. Well, this call was supposed to go until 3:30, but thank you, David. Thank you for joining. We certainly don't have to take all of the way until 3:30, but we can continue.

So the next slide, basically I guess we have had quite a bit of the discussion already, but the idea is we will be sort of bringing back, in the process of identifying and evaluating and selecting the standard we will bring back sort of the other types of standards and another type of approaches that have been used and have been mentioned here. We will then devote some time in the coming calls to evaluate them and determine they're probably based on some of the criteria that we have from the Policy Committee recommendations, as well as other types of criteria, the appropriateness of the standards we're selecting and recommending them to be, the standards for these certificates.

We don't need to get into the discussion in this call. We just wanted to bring it up as this is the first call. We're going to be having a number of additional calls to focus on this in the coming weeks.

Let me go through the next slide. I guess the next three slides are the glossary of terms, so we can certainly have it there as a reference. You will have it and keep it as a reference in the back of your minds.

So let's skip the next two slides and then talk about the timeline and next steps. Can we go to the next slide? One more.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. I'm sorry. I forgot we had these extra. I didn't mean to cut you off here.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
No. That's fine. All right. So, in terms of the timeline for the activities, our goal is to really make recommendations to the HIT Standards Committee, I guess in a first pass and report back to the Standards Committee at the February 16th meeting, probably not the final recommendations, but a report on the status of work. As you all have probably seen or have heard, the Standards Committee is going to be meeting the afternoon of February 16th. There is a day and a half, starting the morning of February 15th and ending at noon on February 16th, a hearing being held by the PCAST Workgroup and the two, the Standards and the Policy Committees have been invited to that.

Then on the second day, the February 16th in the afternoon we will have a Standards Committee when we will be reporting. That first stuff we will do as kind of a first pass, but then we'll finalize and submit our final recommendations by March 29th. The March 29th meeting is the next meeting of the Standards Committee, so that will be sort of our target is in the next couple of months basically to complete our task.

Workgroup meetings: We would need to have a few Workgroup meetings in the next two months. We probably would want to have one in early February. This is something we will be scheduling in the coming couple of days, so one in early February and then one in late February after the February 16th meeting and then one in early March and then a final one in late March if we need to to go with those four workgroup meetings. During those workgroup meetings is when we will be sort of fleshing out, working the details of recommendations for these standards.

I mean this is our primary focus over the next couple of months basically. There might be some additional work of our workgroup on another topic that came from recommendations from the Policy Committee as well, but the topic being the provider directories. It hasn't yet been decided, but there might be some work that the Security and Privacy Workgroup will have to do on that as well, but for now this is sort of our primary focus of attention and this is the timeline that we have laid out, so you will be seeing and receiving confirmation of some of these next conference calls and the times for those.

In terms of the next steps, I think we have identified a number of things here during the call. I'm going to try to summarize some of those. We do want to clarify and make a notation in our materials of the point, John, that you made about the difference between long-term digital signature and just a digital signature for communications here. That's an important clarification point.

We will also bring information around approaches used by the Direct project, the Exchange project. We will look into the federal PKI framework and also look at the VeriSign extended validation search as well and then also probably just pull in from the IHE information that John highlighted. I think we will gather all of that information before our next call and bring it to the group as well.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'd like to make these actions more specific if you don't mind.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. Go ahead.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
What I have is that you, Walter, will find us, track down a copy of the NHIN Exchange specifications for digital certificates. John is going to track down either documents or people, who can give us lessons learned from NHIN Direct. John, is that your understanding?

John
Yes. Not a problem.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. Thank you very much. I told you I would see what I could find more definitive, more clearer and more complete definitions of the classes. Those were the three that I had as real, solid action items.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay. I would add and I can take on that I would add the federal PKI part of it –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, but what's solid about it? I mean it will be covered with NHIN Exchange. NHIN Exchange will have used it. Is there another document or person that you need to track down on the federal bridge?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, because I would not assume that the NHIN Direct project is exclusively or using all of the federal bridge capabilities. I don't think that's the case, so I'll follow up and see when I look into the NHIN Exchange aspect for digital certificates and look at the federal bridge to see if there's any differences that are worth noting.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Excellent. Excellent Perfect. I think that's great. Thank you.

John
Within the NHIN Exchange, Eric Caplan is the Co-Chair of the Security Workgroup and he is actively trying to resolve some issues specifically on the topic you're bringing up, so he can be a contact for sure.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Maybe we should invite him to talk to our group.

John
I think so.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Aaron Caplan is it?

John
Eric.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Eric. I'll remember that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think that would be really the straightest line between two dots there to get us educated on NHIN Exchange and its relationship with the federal bridge. Thank you.

M
Then the individual, I think, for the Direct project really would be Arien. I mean I can represent the word, the writing that I've done in there and I will bring the documents that we've created, but I think to put a face on that and given the experience from the Direct project, Arien would really be the right person.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
He would be a good person to have speak to our group as well, because he could not only address what was decided, but what went into those decision as well. That's a good idea.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes ... I was thinking –

M
David McCallie and I were very involved in those decisions, but it's better to get it from his mouth.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. I agree.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I was thinking about that. I think Arien would be great. We had him talk to us and present at the Policy Committee when we were developing the provider directory recommendations and had him explain the approach that was being used by the Direct project. It was very, very helpful to have him, so have him explain this approaches at the Direct project and the experience with respect to digital certificates will be .... We'll follow up with him and schedule some time for him to come to talk to our group.

Anything else? Any other –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. The other thing I would add; this is Dixie once again; I do see a need for us to clarify the use case or use cases that we're specifying for here, maybe in the use case diagram or however we want to do it, to make rather than just state that we're focusing on communications or in addition to. Are we focusing exclusively, for example, on an NHIN Direct exchange or NHIN Direct plus NHIN Exchange or are we also looking at digital certificates that might be used for SOAP exchanges or REST exchanges or any other kind of authenticated exchanges?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
My sense is and as I read the recommendations from the Policy Committee my sense is that this would apply to any information exchanges of perfected or individual identifiable health information that requires this level of assurance. So I wasn't thinking that this was limited to use cases like NHIN Exchange or Direct, but certainly other exchanges, including things like I'm sending data from my clinic to public health not using Direct or Exchange or the other ... so my sense is this would not be constrained to those two use cases, but basically applied to any instance where there is information exchange for which there is a need to provide this level of assurance.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think we should articulate that. Maybe you could do that in a chart or two or something just to set the stage as this is what we're talking about.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. I was just taking those notes, making those notes as I was talking as well. So yes, in the definition of our scope in the next version of this presentation we'll refine that and clarify that the scope is inclusive of this.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Excellent. That's great. Good. Very good. Thank you, Walter.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Oh, thank you and thank you, everyone, for joining. I'm going to turn it back to you, Dixie. I think we're ready for opening for any public comments, so back to you, Dixie.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, I think we're ready for public comments.

Judy Sparrow – Office of the National Coordinator – Executive Director
Great. Okay. Thank you, everybody. Operator, can you check with the public and see if anybody wishes to make a comment?

Operator
Yes.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. Meanwhile, Dixie and Walter, I'll send you some dates, some suggested dates for February and March –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That sounds good.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay.

Judy Sparrow – Office of the National Coordinator – Executive Director
So we can get it on everybody's calendars ASAP.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Absolutely. Yes.

Operator
We do have a public comment.

Judy Sparrow – Office of the National Coordinator – Executive Director
Oh, great. Thank you. Could you please identify yourself?

Operator
Our next comment is from ....

Judy Sparrow – Office of the National Coordinator – Executive Director
I'm sorry. What is the name?

Operator
Please proceed with your comment.

M
Hello. This is ... from Motorola PKI Center. I appreciate you guys taking public comments. One of my questions was I mean I heard that there is action about the use cases for digital certificates and who is authorized to receive certificates and who is authorized to issue certificates. A lot of these things, to me, are certificate policy issues. Is this group chartered to develop a certificate policy issue that governs these digital certificates?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No. This group is charged with developing standards and we respond to policy recommendations of the Health Information Technology Policy Committee, so I would encourage you to seek, take those concerns to that Committee or to the Tiger Team, which is led by Deven McGraw and Paul Egerman.

M
Okay. If you don't mind, I have a couple of more questions. You also talked about messaging and channel encryption basically, in the ... authentication. I guess encryption is basically a use case for these certificates and I basically wonder if there are any recommendations or requirements as far as robustness rules ... authorities of these keys that are associated with these certificates.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, the use case is not just encryption. It's also authentication.

M
So basically since I saw on the focus of the group that there's certification criteria as well, are there any requirements related to storage of the keys within the machines so they're using these certificates.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That may be part of what we recommend, but our task is to recommend those standards.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. I think it's a good point. I think we will need to think about the implications of the recommendations from the standards side into the EHR certification criteria, because that is certainly another recommendation from the Policy Committee that we develop EHR certification criteria to use in ensuring that EHRs have the capability to handle the certificates. That will be part of the discussions and deliberations we would have I'm sure.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay. Thank you .... Are there any other comments?

Operator
We do not have any other comments at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director
All right. Thank you. Dixie, back to you.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. Thank you, all, for dialing in and to the public for listening in. That's it. Thank you. Thank you, Walter.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. Good-bye.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Good-bye.